10TH INTERNATIONAL COMMAND AND CONTROL RESEARCH AND TECHNOLOGY SYMPOSIUM

THE FUTURE OF C2

# The Harbour Defence IKC2 Experience

Track: Homeland Security

Authors:
Choon Kiat, Tan
Lu Yun, Tan
Jiang Pern, Goh
Teck Hwee, Wong
Lock Pin, Chew

Point of Contact:
Choon Kiat, Tan

Defence Science and Technolgy Agency
1 Depot Road #22-01
DefenceTechnology Tower A
Singapore 109679

Phone : +65 63732338
Fax : +65 62769364
tchoonk1@dsta.gov.sg

# Report Documentation Page

*Form Approved*
*OMB No. 0704-0188*

| | | |
|---|---|---|
| 1. REPORT DATE<br>**JUN 2005** | 2. REPORT TYPE | 3. DATES COVERED<br>**00-00-2005 to 00-00-2005** |

| | |
|---|---|
| 4. TITLE AND SUBTITLE<br>**The Harbour Defence IKC2 Experience** | 5a. CONTRACT NUMBER |
| | 5b. GRANT NUMBER |
| | 5c. PROGRAM ELEMENT NUMBER |
| 6. AUTHOR(S) | 5d. PROJECT NUMBER |
| | 5e. TASK NUMBER |
| | 5f. WORK UNIT NUMBER |
| 7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)<br>**Defence Science and Technology Agency,1 Depot Road #22-01,Defence Technology Tower A,Singapore 109679,DC,20515-6925** | 8. PERFORMING ORGANIZATION REPORT NUMBER |
| 9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) | 10. SPONSOR/MONITOR’S ACRONYM(S) |
| | 11. SPONSOR/MONITOR’S REPORT NUMBER(S) |

12. DISTRIBUTION/AVAILABILITY STATEMENT
**Approved for public release; distribution unlimited**

13. SUPPLEMENTARY NOTES
**The original document contains color images.**

14. ABSTRACT

15. SUBJECT TERMS

| | | | | | |
|---|---|---|---|---|---|
| 16. SECURITY CLASSIFICATION OF: | | | 17. LIMITATION OF ABSTRACT | 18. NUMBER OF PAGES<br>**29** | 19a. NAME OF RESPONSIBLE PERSON |
| a. REPORT<br>**unclassified** | b. ABSTRACT<br>**unclassified** | c. THIS PAGE<br>**unclassified** | | | |

## Abstract

In the past, conventional design of command and control systems has been adopting a client-server approach or the stovepipe structural design, which means that system components are tightly integrated and all system software components have to be completed before the system can be fully operational. Such tightly coupled system architecture imposes rigid limitations on system flexibility for expansion. More crucially, in the rapidly changing environment, it is more important than ever to embrace the evolutionary development process, whereby system components are developed as building blocks, that can facilitate ease of introducing new features within short time cycles.

The Harbour Defence Integrated Knowledge-based Command and Control (IKC2) Experiment was conceived against the backdrop of increasing waves of terror threats. In particular, with the tight coupling of Singapore's prosperity with international trade, protection of our local waters is paramount. This experiment seeks to leverage upon advances in the commercial world to rapidly and cost-effectively deploy solutions to address homeland security, through the Enterprise Architecture approach.

In essence, the experiment seeks to utilise the enterprise architecture approach as a means to achieve the operational vision of IKC2 in the Harbour Defence context. From the integration of sensors to achieve superior situation awareness, to the networking of forces to share a common operational picture, enhanced operationally with the assistance of decision support system. In the experiment, the services provided broadly demonstrate the potential of such a system approach where additional operational capabilities can be introduced progressively, giving the players heightened clarity and an increased situation awareness, thus enabling faster reaction to the situation.

In the paper we will articulate the observations and the benefits that the enterprise architecture provides as well as some pit-falls of adopting Commercial Off The Shelf (COTS) technologies in the context of the Harbour Defence IKC2 Experiment.

## Introduction

There has been an ongoing force-wide effort within the Defence industry to collaborate amongst the different agencies, so as to realise the ‘joint-ness’ necessary for Integrated Command and Control in a network centric environment. In this respect the military had taken many cues from the commercial world, leveraging upon technology that has proven itself in the business and financial arena. The Service Oriented Architecture (SOA) framework in particular holds great promise in the Defence context as it is an effective way for disparate businesses to communicate with each other. Likening the traditional C2 systems of the various Armed Forces Services to business units, a SOA would appear to be a solution to achieving the goal of integration amongst the defence agencies.

## IKC2

The Integrated Knowledge-based Command and Control, or IKC2, framework attempts to holistically define, examine and exploit the information-based revolution in military affairs. This framework was initiated to leverage upon advances in network-enabled and knowledge-based war fighting, to transform the operational capabilities of the SAF and better effect the Integrated Warfare doctrine. A networked force, where each player is a node, overlaps its sensors, shooters and communication nets across the entire battlespace, producing a force stronger than the sum of its individual components.

The Harbour Defence experiment was conceived against the backdrop of increasing waves of terror threats. In particular, with the tight coupling of Singapore’s prosperity with international trade, protection of our local waters is paramount. This experiment seeks to leverage upon advances in the commercial world to rapidly and cost effectively deploy a solution to address this threat. This information-led force transformation, coupled with the pressing need to address both symmetric and asymmetric threats within Singapore’s waters, makes Harbour Defence a good candidate for experimentation.

## Why Web Services are Strategic

There are several ways to implement SOA but the most common implementation is using Web Services. The Harbour Defence Experiment aims to study the feasibility of using a SOA, implemented using Web Services, in developing Command and Control (C2) Systems. In this architecture, the capabilities of a C2 system are packaged as individual Web Services, which are then subscribed by other services to create an integrated service. The aim of this experiment was to explore the feasibility of this idea quickly and at low cost, reusing and modifying existing components where possible.

A Web Service is an URL-addressable software resource that performs functions and provides answers. It takes a set of software functionality and wraps it up so that the services it performs are visible and accessible to other software applications.

Web Services communicate using a flexible, lightweight, and communications transport independent protocol. They are able to inter-operate in a loosely coupled manner by requesting services across the network and waiting for a response.

Web Services can be likened to self-organizing cells that can be combined into new adaptive organisms. Each service exists independently of other services within the network, but they can be combined into larger entities to provide new and better services. By standardising the communication interfaces between the service modules, a service once introduced can be subscribed by any number of network players.

The ability to add on services easily allows the C2 system to be able to adapt to a rapidly changing environment. By following this architecture C2 development is able to embrace the evolutionary development process, where individual capabilities can be developed in parallel and brought online when they are completed. This means a basic or skeleton C2 system can be deployed first, and additional capabilities added on as they are completed. New services can also be introduced with minimal downtime of the entire system. This leads to a faster development and deployment cycle.

## Setup

For the experimental system to deliver meaningful results, it has to be operationally useful to the people for whom it is developed. This meant that a C2 system that conformed to the Web Service architecture had to be built, and it had to possess enough C2 capabilities for the operators to be able to use it as an operational system. The team had to look into the feasibility of compartmentalising C2 capabilities, such as the reception of radar track information, into individual Web Services. For example, in traditional C2 systems, the functionality of receiving tracks from the Radar tracker, processing them and finally displaying to the console were all done within the same application. To make the C2 architecture modular, layers had to be introduced into the C2 system to separate these individual functions, which are then wrapped into separate Web Services. Fig 1. below shows the traditional C2 system model on the left and the Web Service approach on the right.

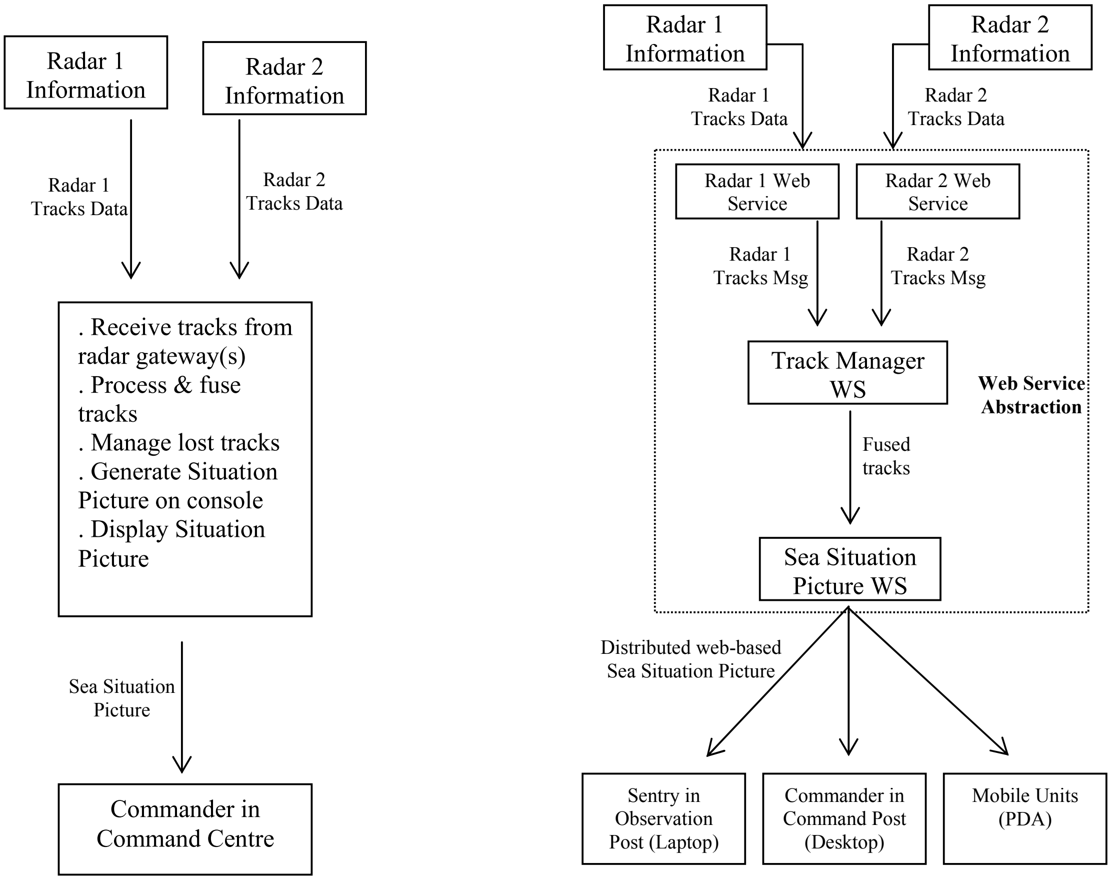


Fig 1.Traditional (Stove-Piped) and Web Service approach to C2 Development

The initial phase was to develop a proof of concept system using components developed as Web Services, followed by the development of a concept prototype based upon this architecture. From the existing C2 system, the radar information was packaged as individual services that would be subscribed and managed by a generic Track Manager Service, a service developed as an aggregator of sensor information. The Track Manager service would then provide the fused track data as a service to any other Web Service that subscribes to it.

## Sea Situation Picture (SSP) Service

A Common Operational Picture constitutes one of the most fundamental services necessary for Integrated Command and Control. To achieve this, the presentation layer was abstracted out of the C2 system as a Sea Situation Picture Service. This abstraction enables the client display to be lightweight, and the service was created with a thin client in mind to facilitate ease of subscription. Clients that wish to access the SSP service need not have any pre-installed software or customisation as the display is available as a web page on the network.

The SSP service subscribes contact information from the Track Service Manager, and provides a consolidated picture that is available on the network. Any user within the Harbour Defence (HD) network, be it a commander or a soldier on the ground, will be able to access the picture within the HD network. Users are also able to perform certain C2 related functions, such as:

- Inserting manual contacts
- Updating of contact status
- Event logging and intrusion logging

This sharing of a Common Operational Picture is instrumental in the co-ordination and collaboration between the players. More importantly, once any player in the network possesses any information on detection, identification or classification of targets, this information can immediately be relayed to all the connected players within the network. This provides an efficient and effective dissemination of information throughout the entire network.

### Networking the forces

For a Service Oriented Architecture to be feasible, there has to be a network in place to link all the players together. In the base context, the wired network only extends links to fixed operational nodes within the base. Networking the forces was achieved by the use of multiple communications options ranging from Digital Subscriber Line (DSL) based on telephone lines to COTS wireless solutions. In the experiment, several wireless solutions were trialled beginning with GPRS due to its island wide reach. The GPRS solution was found to be adequate for the mobile forces, providing a relatively constant throughput of 8 kbps throughout the base, though minor service disruptions are observed during peak periods where the Phone Company bumps off the data channel to make way for voice traffic. Several long range solutions with coverage that extended several kilometres out to sea were trialled, and the team eventually settled on a long range 802.11 (Wi-Fi) solution that provided reliable network coverage within the area of operations of the base defenders.

### Video Imaging Service

Blind spots tend to occur within the area of operations of the base due to natural geographical formations or man made structures. Observation Posts (OPs) are usually erected to cover these blind spots, with sentries reporting any suspicious activity to the base commander. However, voice communications is necessarily slow and provides a low degree of resolution of the situation. The Video Imaging service was introduced to provide a constant video feed at these blind spots to the commander. Installing cameras at the various OPs then distributing the stream from the video servers over the network brings about this service. This implementation of the video imaging service is necessarily constrained by the capabilities of the video server, but still sufficient for the purposes of the experiment. The cameras can also be remotely controlled in a pan-tilt-zoom (PTZ) manner, allowing the base commanders to direct the view where they please.

A similar imaging service is provided for mobile forces.

These imaging services provide the commanders with the ability to be virtually present in any operations that the soldiers undertake on the ground, allowing them to achieve enhanced situation awareness and a superior appreciation of the tempo of operations.

## Own Force Service

The flexibility offered by the Service Oriented Architecture allowed the team to experiment with introducing new services that may be useful to the base users. One important element of the Base Defence force are mobile forces. In the traditional way, sea-based mobile unites are vectored via voice communications with reference to landmarks in the waters surrounding the base. Position reporting of the mobile units to the base commander is also via voice communications and the commander would have to rely on his mental picture of where the mobile units are at any point in time. If more than one mobile units are activated command and control becomes even more difficult.

The team was able to identify several concerns regarding RHIB operations, as follows:

- Vectoring is only with respect to a few reference locations
- Inexperienced sea soldiers sometimes get lost at sea and do not know where they are within the base area
- Where the contact point is not an easily identifiable vessel, vectoring of the mobile unit is via voice communications, which is slow and lacks precision
- Base units have no oversight of mobile units operations in certain areas of the base due to natural obstacles and blind spots

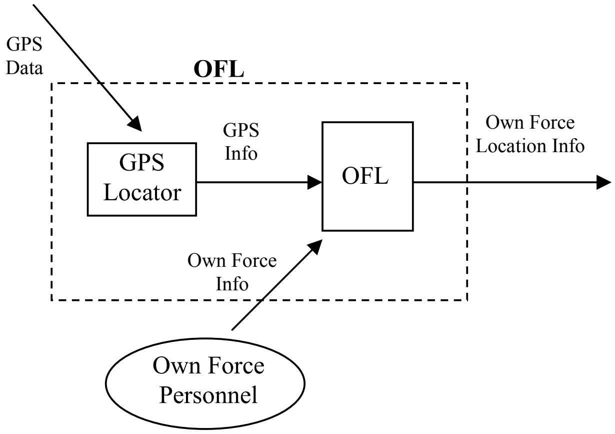


Fig 2. Own Force Locator

The team sought to address these issues by introducing an Own Force Service for the sea soldier. Each mobile unit is equipped with an Own Force Locator (OFL, Fig. 2), an application used to transmit own force information to the Own Force Server (OFS) by pairing a BLUETOOTH GPS device with a Laptop/PDA. The OFL also provides a quick link to the SSP so the sea soldiers are able to view the SSP display. The service was also extended to the QRF jeeps since they perform similar functions on land.

The Own Force Service (Fig 3.) aids mobile unit operations by

- Sending a constant stream of Own Force Location information, consisting of GPS location info and unit info, to the Own Force Server
- Providing mobile unit operators and base units with awareness of their own location within the base at any point in time

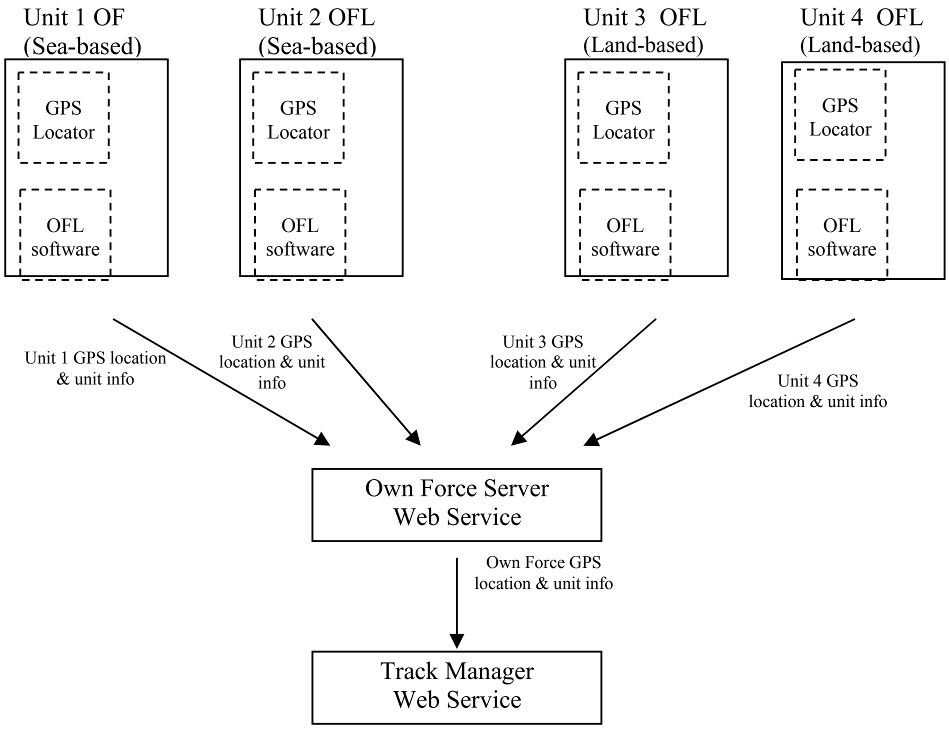

Unit 1 OF
(Sea-based)
Unit 2 OFL
(Sea-based)
Unit 3 OFL
(Land-based)
Unit 4 OFL
(Land-based)
GPS Locator
OFL software
Unit 1 GPS location & unit info
Unit 2 GPS location & unit info
Unit 3 GPS location & unit info
Unit 4 GPS location & unit info
Own Force Server Web Service
Own Force GPS location & unit info
Track Manager Web Service

Fig 3. Own Force Service

The services of the Own Force Server are subscribed by the Track Manager, which packages the own force data together with the track data obtained from the radar sensors and publishes them to the SSP service. In this way the Own Forces are displayed on the SSP as friendly tracks.

## Intent Service – a Knowledge-Based Decision Support System (KbDSS)

The volume of traffic within the sea-lanes can be very heavy, with hundreds of ships crossing the narrow straits at any point in time. Monitoring all these ships can be a daunting task and the sheer volume of information sometimes mask anomalies that may be of interest to the operators. In actual fact, experienced operators monitor the sea picture by searching for behaviour that might indicate something out of the ordinary; in other words, they operate on the principle of exclusion by relying on their tacit knowledge to determine what constitutes anomalous behaviour.

This system has its disadvantages because the efficiency of the system directly correlates with the experience level of the operator, and there is no system in place to effect transfer of knowledge between operators other than training on the job. The intent service was conceived as a decision aid to help the operators sieve out anomalies by capturing the tacit knowledge of the operators as rule sets. This enables the knowledge to be captured in the system for future use. The operators can also update the rule sets once they are familiar with the format of writing the rules. This allows them to fine-tune the system to identify tracks that are anomalous more accurately.

Some capabilities of the Intent service includes

- Detection of non-friendly tracks within Restricted Areas
- Detection of non-friendly tracks approaching Key Installations
- Detection of non-friendly tracks moving out of the Traffic Separation Schemes
- Detection of non-friendly tracks moving irregularly within the Traffic Separation Schemes

## Operational Findings

The HD IKC2 system was trialed for 6 months last year. A survey was conducted with the operators over a period of 1 week to gather feedback about the system. From the feedback, 100% of the operators agreed that the system has improved their appreciation of the sea situation. This result is expected because many operators had no prior appreciation of the sea situation picture before this system. For the commanders to also agree unanimously lends credence to the usefulness of the new services introduced using the SOA.

One concern with the introduction of all these new services was information overload, which might actually have the counter-productive effect of hindering operations. With respect to this concern, 33% of the operators felt the system provided just enough information to assess the sea situation, while 17% and 50% felt the system provided insufficient and too much information respectively. Analysis of this result showed that the majority of those who felt the system provided too much information were the mobile units and base operators. Further discussion with the operators revealed that some features of the system that were relevant to one group of operators were not relevant to another.. This result could be attributed to the clear division of roles played by the base defenders, which a homogeneous picture is unable to address adequately. Though the usefulness of a common operating picture is apparent, the manner in which this picture is distributed to different classes of users to reap operational benefits should be further investigated.

Feedback on the impact the system had on mobile unit operations showed that 65% of them felt the system heightened their appreciation of the tempo of mobile unit operations. In particular, the ability to observe live video feeds from the mobile units improved their ability to assess the situation more quickly. In contrast, the other operators who did not feel the system helped in their operations remarked that the poor picture quality of the cameras made identification of vessels and crew difficult, and the fixed position of the camera meant they had no control over what was being streamed. The team has established that the system was meant to identify if such a video imaging service would be helpful to base defence operations, since this service is not currently available. If the proof of concept proves viable, getting a good feed is just a matter of purchasing a better camera, preferably one that allows remote pan-tilt-zoom control.

## Cons of using Web Services

The addition of layers provide modularity and loose coupling to the system, but the portability of Web Services comes at the price of performance, and this is probably why Web Services have not been more widely adopted in the Defence context. This overhead is incurred mainly due to the need to translate message data into a XML document for sending, which then has to be parsed by the receiving Web Service. Traditional C2 systems that integrate such data exchange within the same application will not incur these overheads. From this we can broadly deduce that Web Service integration will see more application at the strategic level, where response times can range from seconds to a few minutes, and less application at the tactical level. In the Harbour Defence context, the response time required is in the order of seconds, as the base defenders have to be able to react quickly to the threat once it has been identified.

For this experiment, even though the premise is that Web Services are probably better suited for strategic systems, the team decided to be prudent and start on a smaller scale, by targeting services for a tactical C2 system. Since most data exchange is in the form of track messages, and the bottleneck of Web Services lie in the need to marshal these messages into XML documents and back, the messages are pre-cached as XML documents to speed up the retrieval process. A test was conducted to see how many messages could be sent in one request before the delay became too great.

A ‘requester’ and ‘provider’ Web Service each were created and hosted on 2 time-synchronised desktop servers connected within a wired LAN (a single desktop could run both web servers, but the test made use of separate machines to better depict the separation of the services). The ‘requester’ makes a Web Service call to the ‘provider’ for a number of tracks and records the time ($t_1$) at which the request was made. The ‘provider’ receives the request and sends back the pre-cached data corresponding to the request. The ‘requester’ then parses the received message and records the time ($t_2$) at which the XML document is fully parsed. The response time for the Web Service call is then derived by subtracting $t_1$ from $t_2$. Both services are hosted using WebLogic 8.1 application web servers. The results of the test are shown below.

| No of Tracks | Web Service Response Time (mSec) | Web Service with SSL Response Time (mSec) |
|---|---|---|
| 10 | 53 | 82 |
| 50 | 78 | 133 |
| 100 | 136 | 220 |
| 150 | 209 | 287 |
| 300 | 413 | 529 |

From this we can see that the delay incurred in sending 300 track messages between 2 services is around 0.5 seconds. Based on the results of this test the HD team was confident that, given a reliable base network, Web Services could support C2 operations in the Harbour Defence context.

## Pitfalls of using COTS

COTS equipment in general are not meant for use in an outdoor, marine environment. For the purpose of the experiment we have relied exclusively upon the use of COTS products to deliver a proof of concept cheaply, but deployment of an operationally system with similar capabilities would necessitate the use of some military grade components. The following are some of the challenges that had to be overcome during the course of the experiment

- Impact shock of mobile units during high speed manoeuvres
- Doppler effect of fast moving craft on wireless communications
- Strong winds and heavy rain

## Challenges

Beyond these physical challenges, it was also necessary to design the system to be easily used by the sea soldiers. Over the course of the experiment user feedback was gathered on how to make the system more applicable within an operational concept. This was necessary because for the experimental prototype to be able to transit smoothly into Ops usage the users had to be comfortable using the new system, and view it as a tool that aids, not hinder their operations. The lab proof of concept was conducted quite quickly, but many modifications had to be made for the system to be able to be trialled operationally.

For the most part the focus of the experiment has been on enhancing the operations of the mobile units. This is because the mobile units represent the edge of the network within the base defence context. Designing a solution for the mobile units also proved to be the greatest challenge, not only because of the marine environment the mobile units has to operate in, but also due to the physical limitations of the mobile units itself.

The module that underwent the most major iterations was the own force locator for the mobile units. This was in part due to the changing requirements of the project, whereby the communications means was converted to WiFi to achieve a higher throughput.

As most of the equipment used were COTS products, most not even intended for outdoor use much less use within the demanding confines of a fast craft out at sea, weather proofing and ruggedization of the outdoor system was paramount. The objective for the experiment however was not to create a robust solution, but one that could last the operational trials. The impetus of the project then was to come up with answers quickly and cheaply, and the team arrived at various innovative and cheap solutions to effect basic weather proofing of the equipment.

The greatest challenge, however, was in obtaining users to adopt a new command paradigm that essentially delegates responsibility downwards. During the course of the experiment it was noted that processes and reporting procedures continued to be based on the pre-IKC2 system, when information was limited. For a process shift from a command centric to a network centric structure to work, there has to be a corresponding shift in the operating procedures (mental model) of the base defenders. This contributed to the inconclusive results whereby the IKC2 system only marginally improved the efficacy of their operations. A recommendation was made to look into ways to streamline the operations of the base defenders so that the benefits of the IKC2 system could be better exploited.

## References

1. Various Authors, Realising Integrated Knowledge-based Command and Control (IKC2), POINTER Monograph No.2, 2003

2. Patricia B. Seybold , How to Optimize Web Services Investments to Improve Your Customer Experience, An Executive’s Guide to Web Services, Patricia Seybold Group, 2002

3. Robert Eugene Shelton, Using Service Oriented Architecture to Deal with Data and Application Problems, Patricia Seybold Group, 2003

4. Mervyn Cheah, Chew Lock Pin and Tan Chee Ping, Command Control and Information Systems in the Age of Knowledge-Centricity, 2004

10th ICCRTS - The Future Of C2

# The Harbour Defence IKC2 Experience

Tan Choon Kiat

Defence Science Technology Agency, Singapore

# Experiment Objectives

- Observe
  - See first, see more
- Orientate
  - Understand faster and better
- Decide
  - Decide better and faster
- Act
  - Act decisively

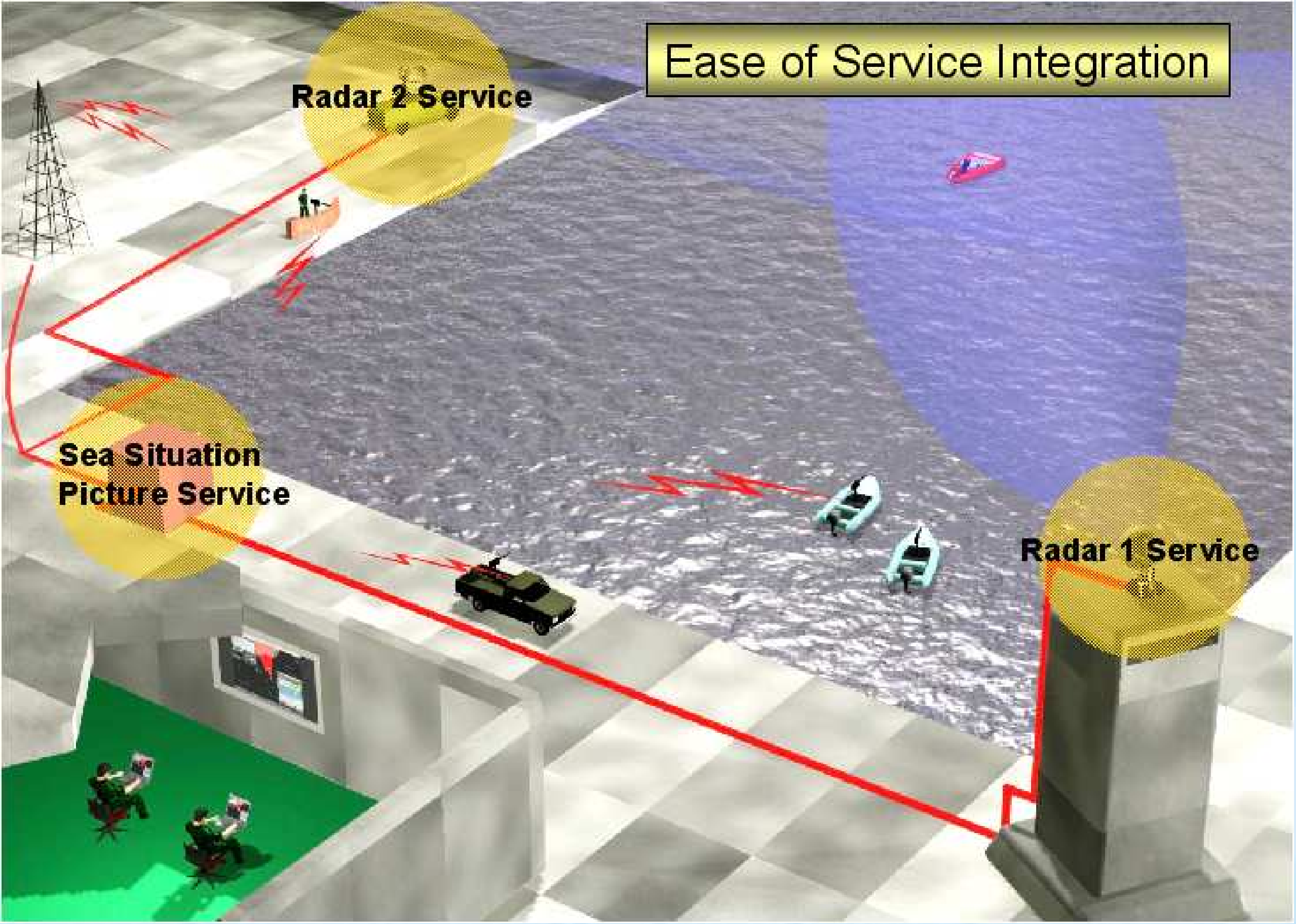
# Experiment Objectives

- Introduce network centric capability using Service Oriented Architecture, to provide interoperability and pervasive accessibility to information and C2 services for all players.

# Design Methodology

- Adopt Web Service as an enabler for SOA
  - Built on top of XML
  - Web service as a wrapper for existing applications
  - Web service abstracts functionality across one or more applications
  - Publishes interface contract in the form of WSDL, an XML format of the service specifications

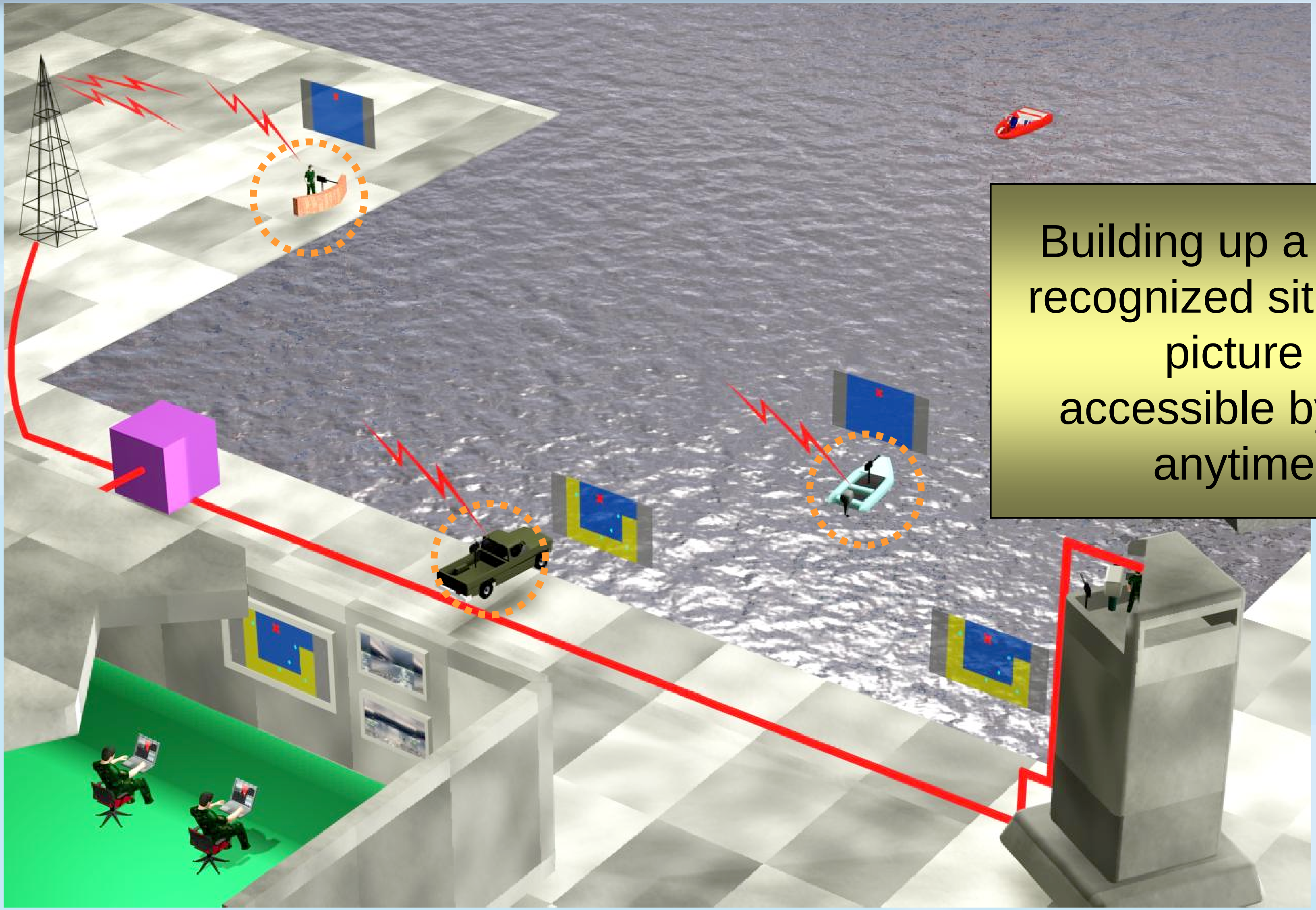
# Web Services Design



# Web Services Design

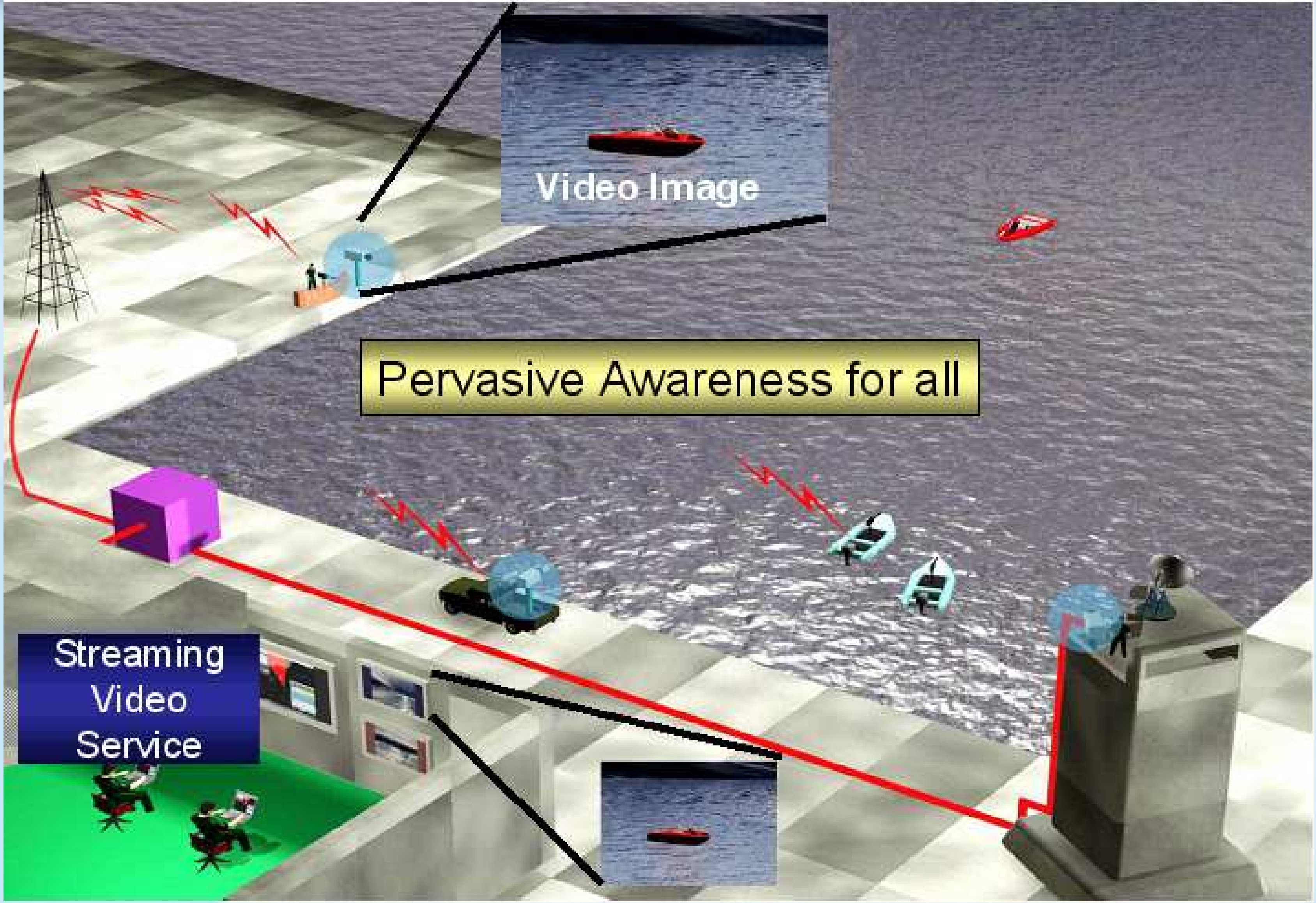
Services Accessibility to all

# Web Services Design



Building up a basic recognized situation picture accessible by all, anytime

# Web Services Design



# Sea Situation Picture Service (SSP)

- Displays and distribute common operating picture to all players in the network
  - Accessible by merely logging on to known URL
  - Situation awareness made available to all by placing remote laptop clients at operational nodes
  - PDA enabled for mobile personnel
  - Allows base defenders to synchronize their actions for faster and better responses to threats

# Track Manager Service

- Aggregates track data from sensors and Own Force Server
- Subscribes to Anomaly data from Intent Service
  - Service of service - able to provide higher service level (anomaly data) if Intent Service is online

# Own Force & Camera Services

- Gets own force unit data from Own Force Locator
- Strategically placed EO/Cameras provide visual picture at commander’s blind spot
- Mobile forces mounted with camera enables commander to assess ground situation as it unfolds
- Commanders to know where his forces are and what they are seeing at that location
- Better resolution of the ground situation

# Intent Service

- Subscribes track data from Track Manager and processes them to sieve out anomalous behaviour
- Aids commander in decision making by sieving out potential threats early
- Existing rules can be periodically reviewed for relevance and new rules implemented according to operational needs

# Observations

Proliferation of Situation Awareness

- Before
  - Situation Picture only at Command Post

- After
  - Situation Picture is available to anyone who is able to tap into the network
  - Forces can be equipped with a PDA and receive the picture on the move

# Observations

## Proliferation of Situation Awareness

- Before
  - Command Post has no real-time knowledge of patrolling units' location
  - Cumbersome communications needed to vector patrolling units and interceptors to scene of action

- After
  - All patrolling units' locations are displayed at all operational nodes
  - With the PDA, patrolling units can coordinate and approach intruder in shortest time

# Observations

## Benefits of Visual Information

- Before
  - Each Observation Post has its own blind spots
  - Identification and verification > 5 min

- After
  - Video streams from various cameras provide visual images to all parties
  - Identification and verification < 1 min

# Lessons Learnt

- Challenges during Lab - Ops transition: e.g. creating experimental environ without impeding operations
- Limitations of COTS - ruggedisation, preventive measures to extend shelf life of equipment needed in marine environment
- Co-evolution of service with Ops users critical to create relevant systems and promote acceptance of system

Thank You